Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/GB05/000978

International filing date: 15 March 2005 (15.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: GB
Number: 0416612.0
Filing date: 26 July 2004 (26.07.2004)

Date of receipt at the International Bureau: 09 May 2005 (09.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/GB 2005 / 0 0 0 9 7 8

INVESTOR IN PEOPLE

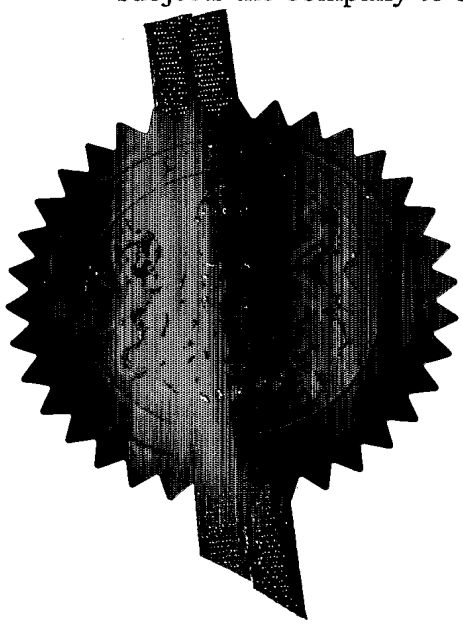
The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



Signed 

Dated 6 April 2005

Pa[redacted]Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

1/77

27JUL04 E[illegible] 123-1 D02000
P01/700 0.00-0416612.0 NONE

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

THE PATENT OFFICE
L
26 JUL 2004
LONDON

The Patent Office
Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference — PDG/DLC/2649301GB

2. Patent application number *(The Patent Office will fill in this part)* — 0416612.0

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Netcraft Limited
Rockfield House
Granville Road
Bath
BA1 9BQ

Patents ADP number *(if you know it)* 8829830001

If the applicant is a corporate body, give the country/state of its incorporation — United Kingdom

4. Title of the invention

Security component for use with an internet browser application and method and apparatus associated therewith

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

MATHYS & SQUIRE
100 Gray's Inn Road
London WC1X 8AL
United Kingdom

Patents ADP number *(if you know it)* 1081001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*
GB	0405901.0	16 March 2004

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	26
Claim(s)	8 DL
Abstract	1
Drawing(s)	6+6

10. If you are also filing any of the following, state how many against each item.

Priority documents	–
Translations of priority documents	–
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	–
Request for preliminary examination and search *(Patents Form 9/77)*	–
Request for substantive examination *(Patents Form 10/77)*	–
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature Date

Mathys & Squire 26 July 2004

12. Name and daytime telephone number of person to contact in the United Kingdom

Peter D Garratt - 020 7830 0000

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

SECURITY COMPONENT FOR USE WITH AN INTERNET BROWSER APPLICATION AND METHOD AND APPARATUS ASSOCIATED THEREWITH

This invention relates to a security component for use with an Internet browser application.

Use of the Internet, and in particular of the World Wide Web (WWW) and e-mail, has increased rapidly in recent years. The World Wide Web is frequently used not only for informational purposes but also for commercial transactions, for example Internet shopping. Internet banking – the online management of financial accounts – has also become increasingly popular. As a result, various forms of computer crime, such as theft of credit card details from e-commerce web sites, and fake or fraudulent e-mails and web sites are also becoming more widespread.

An increasingly common type of online fraud involves criminals who fraudulently obtain sensitive access information such as user names and passwords for online banking services. One way this is achieved is by persuading users to reveal such access information through fake web pages and e-mails. Such web pages and e-mails are typically designed to appear as if they are associated with the relevant bank or other organisation, for example by use of authentic logos and familiar graphical design. Attempts to obain sensitive information in this way are often called "phishing" attacks.

"Phishing" is a name derived from the notion of "fishing for information", and "phreaking", a term used in the 1980's for the process of hacking phone networks and systems to gain access to free calls, or control over parts of the telephony system. In a successful phishing attack, users of online banking services are tricked into disclosing their bank account details, so that the attacker may then log into the their Internet bank and transfer their funds.

Organisations which are not banks, but which have accounts that allow the customer to administer money or other tokens of value are also affected by these fraudulent schemes; this includes credit card companies, credit unions, exchanges, and some Internet retail sites. Amazon, Paypal, Visa, and Ebay are some non-bank sites that have been attacked to date.

Phishing is a highly scalable and attractive opportunity for fraudsters; many people in the civilized world now have Internet enabled bank accounts, and under normal circumstances they offer a more pleasant and more convenient user experience than visiting a bank branch or telephoning a bank call centre. Many businesses also have Internet enabled bank accounts. Accordingly a very significant amount of wealth is accessible via web based banking systems, typically protected by a username and password and other textual tokens supplied over the web by the account holder.

The technology required to construct a phishing fraud is minimal. Conventionally, the fraudster constructs an HTML e-mail message with forged e-mail headers indicating that the e-mail has come from the bank, and asks for the recipient to confirm their bank account username and password. To make the request appear more authentic, the mail usually includes a link to a web server which opens a new window with the bank's own web site (not a copy, but the actual site), and asks for the account details in a separate window, hosted on the attacker's server.

Phishing web sites hosted at reasonably reputable hosting companies will usually be taken down quickly once complaints arrive. Therefore, the attacker's server will often be hosted at a company which is paid to ignore complaints about the fraud; some unscrupulous hosting companies in certain countries are known to sell "bullet proof hosting" as a service, meaning that they will endeavour to keep the site running despite requests to close it down from outside of their own jurisdiction. The attacker's server may also be hosted on a computer that the attacker has broken into, without the owner's knowledge.

There are no dependable, publicly available statistics on how many of a bank's customers receiving phishing e-mails actually respond to them, but the fact that the largest UK banks have taken their entire banking sites offline during some phishing attacks indicates that the fraudsters are enjoying a non-trivial degree of success.

Although, as mentioned above, phishing attacks tend to rely on the visual appearance of fake web sites to fool the victim into believing that the web site is authentic, the URL of the fake web site is also often designed to deceive.

To make the URL appear plausible, attackers conventionally include an "@" sign in the URL, where the text to the left of the "@" is the name of the site to which the victim is expecting to connect, and the text to the right of it is the actual location of the attacker's site.

When the HTTP protocol was originally designed, the "@" character was intended to denote a username at a particular site, as in, for example, "http://sir.tim.berners-lee@www.w3.org", where "sir.tim.berners-lee" is the username, and "www.w3.org" is the name of the web site.

However, URL encoded usernames have never been widely used, with web sites typically using usernames and passwords and/or cookies to administer user sessions and state, and "@" in URLs has almost exclusively been used for tricks, jokes, and fraud attempts.

Recently, a bug in Microsoft's Internet Explorer (TM) became widely publicised whereby if a URL encoded %01 character is placed in the URL it hides a subsequent character from view, as in the following URL used to attack customers of Barclays Bank:

http://ibank.barclays.co.uk%01%01%01%01%01%01%01%01%01%01
%01%01%01%01%01%01%01%01%01%01%01%01%01%01%01%0
1%01%01%01%01%01%01%01%01%01%01%01%01%01%01%01%
01%01%01%01%01%01%01%01%01%01%01%01%01%01%01%01
%01%01%01%01%01%01%01%01%01%01%01%01%01%01%01%0
1%01%01%01%01%01%01%01%01%01%01%01%01%01%01%01@
%77%77%77%2E%6E%65%77%79%65%72%73%6D%2E%63%6F%
6D:%38%30/%31%2C%2C%6C%6F%67%6F%6E%2C%30%30%2E
%70%68%70

The '%01' characters exploits the bug in Microsoft's Internet Explorer web browser, thereby obscuring the appearance of the URL. The encoded characters make it difficult for recipients to spot the "@" sign that gives away the concealed URL of the target web page. In the above example, the URL the user sees displayed in the browser window will be "http://ibank.barclays.co.uk", whereas the real URL of the web page being viewed is actually "http://www.newyersm.com:80/1,,logon,00.php".

Internet browser applications typically display an indication of whether a web page being accessed is "secure", that is to say, whether communication between the browser and the web server is encrypted. For example, the browser window of Microsoft's Internet Explorer (TM) comprises a status bar which, amongst other things, displays a lock symbol when an SSL web site is being accessed. However, this information only indicates that the communication between the browser and the server is protected. Furthermore this information can easily be missed or ignored by the user, who may not be aware of its significance. A user is particularly likely to fail to notice the absence of the lock symbol when visiting what appears to be a very familiar web site. Furthermore, if a fake web site is implemented as an SSL site, the lock symbol would be displayed, reassuring the user into believing that the site is safe.

As mentioned above, in some fraudulent schemes the authentic web site of the financial institution is displayed, with a pop-up window requesting the relevant information. Since pop-up windows are frequently displayed without window features such as toolbars and status lines, the user might believe they are accessing the authentic website although the pop-up window is in fact not associated with the authentic SSL site displayed behind it.

It is therefore an object of the present invention to alleviate some of the above problems.

Accordingly, in a first aspect of the invention, there is provided a security component for use with an Internet browser application which displays Internet resources in response to receiving resource locators specifying the Internet resources; the security component comprising means for receiving a resource locator from the browser application and means for providing a security alert if the resource locator fulfils one or more criteria.

In this way, users can be provided with improved security when accessing resources on the Internet.

The Internet browser application may, for example, be a web browser for browsing the World Wide Web. The term "Internet resources" preferably includes any type of resource available on the Internet, including web pages (for example in HTML format), and other document and media files, such as

audio and video data files. Resource locators may, for example, be in the form of Uniform Resource Locators (URL). Resource locators may also be in the form of encoded representations of URLs. For example, part or all of the URL may be encoded as a check sum or hash code.

Advantageously, the component further comprises means for comparing the resource locator to a character pattern. In this way, resource locators containing unusual or suspicious characters can be identified, leading to improved security. The component preferably further comprises means for transmitting a representation of the resource locator to a security information server, and means for receiving security information relating to the resource locator from the security information server. This can provide a more flexible way of obtaining security information relating to a resource locator. The representation of the resource locator may simply be the resource locator itself, or may be an encoding of the resource locator, comprising, for example, a check sum or hash code of some or all of the resource locator. The security information may suitably comprise an indicator indicating whether the resource locator has been identified as being associated with a potential security risk, in which case the criteria may comprise the indicator. In this way, suspicious resources can be more easily identified. To further enhance the security, the alerting means may be adapted to prevent the Internet browser application from displaying the Internet resource specified by the resource locator.

In a further aspect of the invention, there is provided a security component for use with an Internet browser application which displays Internet resources in response to receiving resource locators specifying the Internet resources; the security component comprising means for receiving a resource locator from the browser application; means for transmitting a representation of the resource locator to a remote server; means for receiving IP registration information relating to the resource locator from the remote server; and means for displaying the IP registration information. This can enable a user to better judge the security of a resource to which a resource locator refers.

In a further aspect of the invention, there is provided a security information server comprising: a database of security information relating to

Internet locations; means for receiving a security information request comprising a representation of a resource locator from a user terminal; means for retrieving security information relating to the resource locator from the database; and means for transmitting the security information to the user terminal.

In this way, a more efficient way of managing and distributing security information can be provided. The term "Internet location" preferably refers to an Internet domain, sub-domain or host, to an IP address, to an Internet page or Internet site, or to any other suitable Internet information source unit.

Advantageously, the database may be adapted to store a list of representations of resource locators having been identified as being associated with a potential security risk, the security information server further comprising means for comparing the received resource locator representation to the stored list of resource locator representations, the transmitted security information comprising an indicator indicating whether the received resource locator representation matches one of the stored list of resource locator representations. This can allow easier identification of potentially dangerous resources.

The database is preferably adapted to store information relating to suspected security vulnerabilities associated with an Internet location. This can enable a more accurate assessment of the security of an Internet location. For the same reason, the database is preferably adapted to store registration information relating to a plurality of IP addresses, and the retrieving means is adapted to retrieve registration information relating to an IP address associated with the received resource locator representation.

In a further aspect of the invention, there is provided a method of providing security information comprising: receiving a representation of a resource locator relating to an Internet resource requested by a user of an Internet browser application; and alerting the user if the resource locator fulfils one or more criteria.

In a further aspect of the invention, there is provided a method of providing security information to a user accessing via the Internet accounts for holding or managing money or other tokens of value, comprising: storing domain names and/or IP address information relating to trusted Internet sites

providing access to such accounts; receiving a resource locator specifying an Internet resource requested by the user; determining whether the resource locator relates to a trusted Internet site by comparing a domain name or IP address associated with the resource locator to the stored domain names and/or IP address information; and outputting a corresponding indication to the user if it is determined that the resource locator does relate to a trusted Internet site.

The invention also provides a plug-in or toolbar for an Internet browser application comprising a security component as described herein and/or adapted to carry out a method as described herein.

The invention also provides a computer program and a computer program product for carrying out any of the methods described herein and/or for embodying any of the apparatus features described herein, and a computer readable medium having stored thereon a program for carrying out any of the methods described herein and/or for embodying any of the apparatus features described herein.

The invention also provides a signal embodying a computer program for carrying out any of the methods described herein and/or for embodying any of the apparatus features described herein, a method of transmitting such a signal, and a computer product having an operating system which supports a computer program for carrying out any of the methods described herein and/or for embodying any of the apparatus features described herein.

The invention extends to methods and/or apparatus substantially as herein described with reference to the accompanying drawings.

Any feature in one aspect of the invention may be applied to other aspects of the invention, in any appropriate combination. In particular, method aspects may be applied to apparatus aspects, and vice versa.

Furthermore, features implemented in hardware may generally be implemented in software, and vice versa. Any reference to software and hardware features herein should be construed accordingly.

Preferred features of the present invention will now be described, purely by way of example, with reference to the accompanying drawings, in which:-

Figure 1 gives an overview of the architecture of a security system;

Figure 2 illustrates the security system of Figure 1 in greater detail;

Figure 3 is a simplified representation of the visual appearance of a web browser window using a security toolbar;

Figure 4 is a simplified representation of the visual appearance of the security toolbar of Figure 3;

Figure 5 is a flow diagram illustrating the processing performed by the security toolbar; and

Figure 6 is a flow diagram illustrating the processing performed by a security information server.

Overview

The proposed security system takes the form of an extensible and adaptive web based database system. It is intended to defeat a popular form of fraudulent attack on web based banking systems, and also provide significant ancillary benefits in the form of additional security, an Internet-wide community or neighbourhood watch scheme, and considerably enhanced marketing opportunities.

The security system is illustrated in overview in Figure 1.

A plurality of user terminals 10 (for example, general purpose personal computers) are connected to a network 16, in the present example the Internet, through which they can access a variety of information. An Internet browser application 12 (also referred to simply as a web browser) is provided on each terminal to manage the access to the resources available through the Internet, in particular via the World-Wide Web.

Associated with each web browser 12 is a security component 14. A security information server 18 is also connected to the Internet.

The security component 14 interacts with the web browser to provide security information to the user of the browser regarding web sites visited by the user. In particular, the security component 14 performs a number of checks on any URL (Uniform Resource Locator) entered by the user. Firstly, the component 14 performs local checks to determine whether a URL matches certain criteria. Secondly, the component carries out remote checks by communicating with the security information server 18 via the Internet 16.

The security information server 18 stores information relating to the security of web sites on the Internet, which can be sent to the security component 14 on request. Furthermore, the user of the security component 14 can provide security information to security information server 18, in particular by reporting web sites that the user considers to be suspicious. Such user feedback is stored in the database and is then available to other users of the system.

In a preferred embodiment, the security component 14 comprises a toolbar which can be integrated into the web browser application 12.

Toolbars are software components which provide a grouping of user interface features such as selection boxes, input fields and buttons, along with associated functionality. Toolbars can be provided as add-in components (also called "plug-ins") to existing software applications to enhance the applications' functionality. For example, web browsers such as Netscape Navigator (TM) and Microsoft Internet Explorer (TM) allow toolbars to be installed as part of the browser to perform additional functions that the browser's creator has considered too specialised to implement natively within the browser itself.

Examples of toolbars available for Microsoft Internet Explorer (TM) include the Alexa toolbar (developed by Alexa Internet) and the Google toolbar (provided by Google, Inc.).

As described above, the toolbar provides both local and remote checking of URLs requested by the user.

Local checking involves determining whether the URL conforms to certain criteria. In particular, this involves detecting suspicious characters or character patterns which might indicate that the URL is associated with some kind of fraud attempt. The "@" and "%01" characters discussed above are examples of such characters.

The toolbar can trap these suspicious URLs, and highlight them as dangerous. It can further report such URLs to a central database managed by the security information server 18, from where they can in turn be reported to the bank and hosting locations as appropriate.

Instead of using URLs encoded in particular ways as described above, attackers may use other methods to create URLs which appear reasonably

authentic, for example by using domain and/or host names which are textually similar to those of the bank or other organisation.

To address this, and to provide additional benefits, the toolbar further carries out remote checking against a database of security information held by the security information server 18. To achieve this, the toolbar reports each URL visited by a user to the central database. If the reported URL is one which has been reported as suspicious by other users, this is immediately reported back to the toolbar, and a suitable warning message is then displayed.

The very fact that phishing attacks are usually carried out on a large scale (that is, the attackers will typically send many thousands or even millions of e-mails in the expectation that some will reach customers of the bank), means that the chance of a fraudulent web site being reported quickly is increased, which in turn expedites reporting of the fraud attempt to the bank or other organisation, its customers, and hosting locations. The users of the toolbar are effectively mobilised into a large cooperative watch scheme, where once the first recipients of the fraud have reported it, this information is available to other recipients of the attack as they access the URL.

Implementation

The implementation of the security system will now be described in more detail with reference to Figure 2.

As described above, the system comprises two main components: a security component that resides on each user computer and is active whenever the user is browsing the web using web browsing software (implemented, in the present example, as a toolbar) and a security information server including a database, which must be able to respond quickly to large numbers of requests as each of the system's users moves around the world-wide web.

Toolbars are typically implemented using an API (application program interface) made available by the web browser provider, and/or toolbar building toolkits available from third party suppliers.

The central server (in practice, this can comprise multiple computers, potentially spread over multiple locations; it will be referred to herein simply as the central server, as it is a logical unit of functionality) maintains information

on the state of the user community and the system's knowledge about URLs and sites visited by the community.

Communication between the toolbar and the central server uses the HTTP protocol, as well as the SSL protocol (which is essentially encrypted HTTP) for any information where the sensitivity merits the computational overhead of the encryption operations.

Much of the functionality of the system could in principle be performed either on the users' local machine by the toolbar, or by sending data to the central server. The location of the processing is decided by efficiency considerations.

As described above, user terminal 10 communicates with central server 18 via the Internet 16 in order to obtain security information relating to URLs visited by a user of the user terminal.

Specifically, the user terminal 10 comprises a web browser application 12, for example Microsoft Internet Explorer (TM) or Netscape Navigator (TM). The toolbar component 14 is associated with web browser 12 and communicates with the web browser to provide security information. The toolbar component 14 maintains a pattern store 22, for storing one or more character patterns used to identify suspicious URLs.

Central server 18 manages a security information database 20 which stores security information relating to web sites.

In use, a user enters a URL into web browser 12 (for example by keyboard input or by clicking on a link). Before displaying the requested web site, the web browser 12 passes the URL to the toolbar component 14 for checking. The toolbar performs both local and remote checks to determine whether any security risks are associated with the URL entered.

Firstly, the toolbar component attempts to match the URL against a number of character patterns stored locally in pattern store 22. The character patterns may, for example, specify particular characters or character sequences whose appearance in a URL may indicate a security risk. If the URL matches one of the stored patterns, the user is alerted by display of relevant information in the toolbar, and the toolbar instructs the browser 12 not to proceed with loading the web site specified by the URL but to display suitable warning information instead. The URL is thereby effectively blocked,

though the user is given the opportunity to override the blocking and access the blocked site if required.

Secondly, the toolbar sends a token representing the URL via the Internet to security information server 18. The representation of the URL may simply be the URL string itself. However, for privacy reasons, it may not be desirable to report each URL in full to the security information server 18. In preferred embodiments, the toolbar therefore transmits an encoded representation of the URL. The encoded representation comprises the host and domain level information from the URL in clear text, together with a check sum or hash code of the remainder of the URL.

For example, the URL "http://www.example.com/users/private" would be transmitted to the security information server as "http://www.example.com" in clear text together with a hash code or check sum of the remainder "/users/private". The check sum or hash code may be generated using any suitable algorithm. Alternatively, a check sum or hash code of the entire URL could be used.

This ensures that sensitive personal information which is often contained in URLs is not recorded by the security information server.

Other suitable representations of URLs may also be used, and any reference herein to resource locators or URLs shall be taken to refer also to any such representations of resource locators or URLs, as is appropriate in the context.

Security information server 18 looks up the representation of the URL in security information database 20 and returns any relevant security information relating to that URL. If the URL has previously been identified as potentially dangerous, then the central server instructs the toolbar component 14 to block the web site as described above. In any case, further security information is also transmitted to the toolbar if available, including information regarding known vulnerabilities and information relating to the hosting location of the URL.

This information is displayed by the toolbar 14. Then, if the URL is not to be blocked, the toolbar instructs the web browser 12 to retrieve the relevant web site. The web browser then loads and displays the requested page.

The toolbar

The toolbar will now be described in more detail with reference to Figures 3 to 5.

Fig. 3 illustrates, in a simplified manner, the visual appearance of a web browser using a security toolbar as described herein.

The web browser executing on the user terminal displays a browser window 40, including common browser interface components such as a menu bar 42, an address bar 44 for entering and displaying URLs, a browsing toolbar 46 containing buttons for standard browsing functions such as *back*, *forward*, *stop* and *home*, and a page display area 48. The user accesses a new web page typically either by entering a URL into address bar 44 or clicking a link in page display area 48 (other ways of selecting web pages may also be provided, for example by way of a "favourites" menu or history list). The web browser then fetches the web page corresponding to the URL entered and displays it in display area 48. The security toolbar 50 provides functions relating to URL checking and security information display.

Figure 4 illustrates the appearance of the toolbar in more detail, again in a simplified manner and purely by way of example.

Toolbar 50 comprises a logo display area 52 for displaying a name, logo or other indication of the toolbar provider. This may, for example, be a financial institution. In the present example, the (fictitious) name "FakeBank" is shown.

The toolbar further comprises a button 54 for reporting a suspicious web site and a further button 56 for requesting further security information relating to a web site. In the example, these are labelled with an exclamation mark and a question mark respectively, but they may of course be labelled with any suitable graphic or text label or a combination of the two.

A status display area 58 of the toolbar 50 provides a summary of the security status of the web site currently being accessed, stating whether any known security vulnerabilities are associated with the web site (60) and giving the country (62) and name (64) of the company to which the IP address corresponding to the URL is registered.

They toolbar may also provide further functions, for example by way of further buttons or by way of a menu accessible by right-clicking on the toolbar.

The toolbar receives an event notification from the web browser when the user requests a new URL. As previously described, the toolbar then performs both local and remote checking on the URL, firstly by pattern matching against locally stored character patterns and secondly by obtaining security information from the security information server.

Upon receiving the event notification stating that a new URL has been requested, the toolbar attempts to match the URL against patterns of dangerous URLs. These patterns are supplied to the toolbar by the security information server. In principle, patterns can be maintained through a general software update mechanism (as described below), or through a separate protocol of request/responses to the security information server.

Since the number of patterns is likely to be small, and change relatively infrequently, it is likely to be more efficient to perform this pattern matching locally on the user's computer, with the toolbar polling the security information server for updates to the patterns when the web browser application starts up.

As mentioned above, phishing attacks often involve opening the authentic web page of the bank or other organisation in the background, with the fake web page relating to the attack displayed in the style of a pop-up window in front. The pop-up window will usually suppress display of the menu bar, address bars and toolbars that are normally displayed in a browser window (as is usually the case for advertising pop-up windows and the like), so that the user cannot see the URL of the page being displayed and is led to assume that it, like the bank's web page behind, is authentic. Naturally, the user would also be unable to see the security toolbar in this case.

A further feature of the toolbar is therefore that it forces display of at least the address bar and security toolbar in every browser window, including pop-up windows.

The processing performed by the toolbar is summarised in Figure 5.

At step 102, the toolbar receives a URL from the web browser for checking. At step 104 the toolbar compares the URL to the character patterns stored in the pattern store. If a match is found, then an alert is displayed and the web page referred to by the URL is blocked at step 106.

A representation of the URL is then sent to the security information server in step 108. The toolbar receives a response from the security

information server at step 110 in the form of security information relating to the URL. If the response indicates that the URL relates to a web page which has been flagged in the security information database as potentially dangerous, the user is alerted and the page is blocked (step 112). In any case, the security information received from the security information server is displayed (in the status display area (58) of the toolbar) in step 114.

The alerting of the user and blocking of the web page is achieved by instructing the browser to display a warning page in place of the actual web page referred to by the URL. The warning page may, for example, include a message that the page has been blocked and why, a link via which the user can report that the web page has, in the user's opinion, been incorrectly flagged as dangerous, and a link via which the user can gain access to the blocked page despite the security warning.

If the local and remote checks did not indicate that the web page should be blocked, then the web browser retrieves and displays the requested page as normal.

In addition to its primary security-related functions, the toolbar also provides the following additional functionality:

Version management: On start up the toolbar checks with a software update server to determine whether a new version of the toolbar is available, and offers to download and install the new version if this is the case (the software update server may be incorporated into the security information server or may be separate).

Branding: The toolbar can further provide branding and navigational functionality relevant to the toolbar provider. For example, the provider of the overall security system and of the toolbar software could licence the toolbar and reporting functionality to organisations such as banks, financial institutions, and e-commerce companies, offering them the ability to brand the toolbar with their own logos, brands and identifying marks, to provide shortcuts to their own services and to bring new information and offers to the attention of its customers via the toolbar. Such licensees would typically pay an annual licence fee for the services provided, for example based on the number of customers of the licensee using the services.

In this way, in addition to the fraud fighting attributes which would reduce financial loss to the banks or e-commerce sites and their customers, the toolbar can therefore provide an attractive branding and customer loyalty mechanism for the provider, keeping their logo and services on screen throughout the time the customer spends using the web.

Licence management: For commercial flexibility, the opportunity to grant licences to organisations covering a particular time frame may be desirable. This can be achieved by providing licence management functionality, whereby the toolbar checks with a central server (such as the software update server described above) on start up to determine if a licence period has been exceeded, and disables the toolbar if it has.

Tell a friend: The system provider may wish to encourage deployment of the toolbar to proliferate as quickly as possible. In this respect, the toolbar could include "Tell a friend" functionality to enable users to more conveniently recommend its adoption to their friends and colleagues, for example by way of automatic e-mailing to one or more e-mail addresses entered by the user.

The security information server

The security information server will now be described in more detail with reference to Figures 2 and 6.

As shown in Figure 2, the security information server 18 manages the security information database 20, which stores various types of security information relating to web sites and web pages.

The security information server 18 further processes security information requests received from toolbars.

Each such request includes a token representing a URL which is to be checked by the security information server. The server compares this URL representation with a list of potentially dangerous URLs previously reported by the system's user community, which is stored in the security information database. The URLs may be stored in a representation corresponding to the representation of URLs received from the toolbars, in which case a direct comparison is performed. Alternatively, the database may store reported URLs in clear text, in which case the comparison step comprises generating the equivalent representation (including the check sum or hash code) of URLs

in the list and comparing the generated representation to the URL representation received.

Normally the results of this comparison will be negative, in which case the browser continues its normal action. However, if the user requests a URL which appears in the list of potentially dangerous URLs, then the security information server notifies the toolbar of the match, and the toolbar alerts the user to the circumstances.

Three main types of security information are managed by the security information server: user reporting information; hosting location information and vulnerability information. These will now be described in more detail.

User reporting information: As described above with reference to Figure 4, the toolbar 50 comprises a button 54 for reporting web sites believed to be in some way suspicious. When a knowledgeable and experienced user visits a previously unreported URL that he believes to be related to a fraud such as a phishing attack, he can report this using the reporting button on the toolbar. The security information server then records this information against the URL and may additionally flag the URL for review, highlight it as a threat to any other community members visiting the URL, or wait for corroborating reports from other members of the community, or review from a system administrator.

Additionally, to deal with mistaken or malicious reporting of benign URLs, the user may also be given the capability to report any URL that he thinks has been incorrectly classified as dangerous. As the volume of reports requires, user identifiers can be allocated for reporting users so that past reliability of reporting can be used to corroborate future reports.

Because of the financial importance of the information, each reported URL would typically be inspected by a system administrator and, if validated, reported to the appropriate bank, hosting location, and law enforcement agency. The system administrator has the ability to outvote any and all reports on given dangerous URLs, as once the system becomes widely adopted, it is conceivable that fraudsters could register as users of the system to affect the user feedback concerning their own URLs.

Hosting location information: Additionally, the security information database stores information relating to the hosting location of web sites.

More specifically, the database stores IP registration information relating to IP addresses, which includes information indicating the company or person to whom a given IP address is registered. For a given URL, the IP address of the host on which the web page referred to by the URL resides can be determined by DNS server lookup. Registration information relating to that IP address can then be obtained from the security information database. By displaying this information on the toolbar the victim of an attack can immediately see that the IP address of the web page he is visiting – which appears to be associated with his bank's real web site – is not actually registered to his bank (and is potentially even registered in a different country).

The registration information for IP addresses is obtained from the various IP address registries worldwide, typically in the form of regular snapshots of the registries' registration data (for example on a daily or monthly basis). This information can be used to derive the registered owner and country of each IP address on the Internet.

For efficiency purposes, instead of automatically retrieving this information and forwarding it to the toolbar for display in response to a request, an additional button could be provided on the toolbar via which the user can specifically request this information.

If the site being viewed is in the DNS (Domain Naming System), the user can also be given the option of requesting the system to look up the domain name registration details of the site's domain, as corroborating evidence that the site is not, in fact, related to his bank.

Vulnerability information: The security information database also stores information relating to security vulnerabilities which are believed to be present in particular web sites. Vulnerabilities are typically weaknesses or bugs in operating system and web server software which can be exploited by attackers.

Fraudulent activities such as phishing attacks are sometimes run from compromised servers without the knowledge of the server's owner. Knowing whether a web site has security vulnerabilities (and therefore might be under the control of a criminal) can therefore be helpful to the user.

Additionally, the general security of Internet commerce sites is much poorer than a layman might reasonably expect, with many commerce sites operating on versions of software widely known to be vulnerable.

As an example, some criminals have been known to break into e-commerce sites, and install monitoring programs to record financially useful information such as credit card and bank account details as they are entered into the site. Honeynet, a consortium of Internet security administrators, have shown that the carding community (a community of criminals operating in this field) operate exchanges where control of compromised e-commerce sites is traded along with actual card details harvested from the sites, while according to the UK banking association APACS, Internet card fraud grew by 86% during 2002.

Knowing that a site is likely to be vulnerable would be useful for the user to help identify sites that might be under the control of criminals, or where criminals might easily obtain control in the near future. Displaying information relating to known security vulnerabilities can therefore also aid a user in making an informed decision as to whether to trust the security of a commercial web site before supplying sensitive information such as credit card details to it.

It is generally not practical for the system to extensively test sites for security vulnerabilities, as this is indistinguishable to the site from an actual attack. However, it is reasonable for the system to interpret information conventionally published by the site, to see if this contains any information that might indicate that the server is vulnerable. Information in this class would include the name of the web server software and the software version, the type and version of the operating system, any of the web server module names and versions, and any information that can be determined from retrieving the front page of the site.

Some "false positive" reporting (where the site has actually patched a security vulnerability, but continues to publish a version number that is known to be vulnerable) is likely to occur when the recommendation is primarily based on product and version information published by the site. However, some well known credit card, banking and commerce web sites have the security of their sites tested in depth by specialist Internet security firms, and

for these sites, any such additional information available can be added to the security information database to give a more accurate opinion on the site's security. Such information may then give users an extra degree of confidence in the security of the web sites in question.

To obtain vulnerability information, the security information server examines each web site which has in the past been accessed by members of the user community and compiles an assessment of its security using information that it maintains relating to known vulnerabilities of web server and operating system software.

It is generally preferably to wait until a community member accesses a given page before analysing it for security vulnerabilities, since there is no need to evaluate a web site that is not visited. A timestamp is taken at the point of the evaluation and this is stored together with the results of the evaluation so that the information can be stored for a suitable period (say 24 hours) before considering whether it should be re-evaluated. Due to the large number of web pages that would potentially need to be evaluated, a performance gain could be achieved by limiting the number of pages taken from any one web site (for example, by taking a logarithmically decreasing sample after the first 100 distinct page requests relating to a given web site).

Assessments are primarily formed using rules which apply to the web server headers and page content visible on a conventional page request, but could additionally include information from knowledge of previous site security breaches (obtained, for example, from defacement archives), and other security testing services where used by the web site in question. Users can thus be presented with an informed opinion on the security of the web sites they are visiting.

Although the security vulnerability information relating to a given URL could be obtained dynamically by carrying out a vulnerability assessment in response to a request received from a toolbar, for efficiency and performance reasons it is preferable to perform assessments independently of the requests and to store the resulting vulnerability information in the database. For example, the security information server could perform vulnerability assessments on a daily basis, assessing any new web sites visited by users during the last day, as well as any existing web sites for which vulnerability

information is already stored in the database, but which are due to be re-evaluated. Alternatively, the security information server could perform a dynamic vulnerability assessment only on those web sites for which information is not already available in the database.

As mentioned above, the hosting location information and vulnerability information associated with a URL is transmitted to the toolbar where it is displayed. Specifically, the toolbar displays a summary of the vulnerabilities found (possibly none), as well as the hosting location information (company name and country). If the web site in question is one which has been more fully tested, or for which no vulnerability information is available yet, then this is also indicated. Vulnerabilities may be classified according to severity, for example into *problems* and *warnings*, with *problems* being security vulnerabilities which could allow hackers to gain access to or control of the web server (and hence access to personal details stored there), and *warnings* being less severe vulnerabilities, for example relating to the possibility of Denial of Service attacks. The summary presented by the toolbar might then give the number of vulnerabilities of each type found, and provide the user with the option of viewing details of the vulnerabilities (using the information button 56 as shown in Figure 4). In the example of Figure 4, the status display area 58 of toolbar 50 indicates that no known vulnerabilities are associated with the present web site (60) and that the IP address of the page being viewed is registered to "FakeBank plc." (64) in Great Britain (62).

The processing performed by the security information server in response to an information request received from a toolbar is summarised in Figure 6.

At step 202, the security information server receives a request containing a representation of a URL to be checked. At step 204, the server compares the URL representation to a list of potentially suspicious URLs (as reported, for example, by other users) stored in the database. In case of a match, an alert is transmitted to the toolbar at step 206.

At step 208, the server performs a DNS lookup to determine the IP address associated with the URL (this being the IP address of the host referred to by the URL). It then retrieves IP registration information relating to the IP address from the database in step 210, in particular the name and

country of the company to whom the IP address is registered. The country can, for example, be derived from the dialling code of a company telephone contact number given in the registration information, if the registration information does not itself indicate the country.

At step 212, the server retrieves vulnerability information relating to the web site from the database. This may be recorded in the database either against the domain and host name or the IP address of the web site referred to by the URL and looked up accordingly.

A response comprising the security information is then transmitted to the toolbar at step 214, where the information is displayed to the user.

Although the alerting step 206 has been described above as a separate step, the alert may actually be transmitted as part of the response sent at step 214.

In a preferred embodiment, the security information transmitted at step 214 is only a summary of the information available in the database. For example, the security information server may simply indicate whether or how many security vulnerabilities are associated with a given web site. By way of an information button on the toolbar (item 54 of Figure 4), the user can request more detailed information, such as the exact types of vulnerabilities detected. Due to the limited screen space available to the toolbar, this detailed information may, for example, be displayed in the form of an HTML page in page display area 48 rather than in the toolbar itself.

In some embodiments, as an alternative or in addition to the information described above, the security information database 20 (shown in Figure 2) may store a "safe" list of trusted banking-related web sites, in the form of lists of domain names and/or IP addresses or IP address ranges which are known to be registered to genuine banks and similar financial institutions. This safe list can be used to provide a "safe Internet banking" icon which is displayed on the toolbar whenever a trusted banking-related web site is visited by the user.

In a preferred embodiment, the security information database 20 stores both a list of known domain names and a list of known IP address ranges registered to banks and other financial organisations. When the security information server 18 receives a security information request from a toolbar

including a URL (or a representation of a URL as described above), it compares the domain name of the URL to the list of known domain names stored in security information database 20. It also performs a DNS lookup to obtain the IP address associated with the URL as described above, and compares the IP address to the list of known IP address ranges stored in the database. The security information server then reports its findings back to the toolbar.

If the domain name or IP address was found in the relevant list, the toolbar then displays a graphical icon indicating that the web site being accessed is known to belong to a trusted banking organisation. This can give the user greater confidence that the web site being accessed is genuine and safe. The icon may be displayed if either the domain name or the IP address can be matched, or may only be displayed if both domain name and IP address can be matched. If neither the domain name nor the IP address are found in the database (or alternatively only one of them), then the icon is not displayed. If the user believes that he is accessing a banking web site, then the absence of the graphical icon in the toolbar should alert the user to the fact that the web site being accessed is not known to the system and therefore may not be genuine. Alternatively, a negative indication could be displayed.

The banking organisations themselves can educate their customers to check that this "safe banking" icon appears in the toolbar before providing any personal details or otherwise attempting to use a (supposedly) banking-related web site.

Before the system is first used, the database is populated with details of the domain names and IP address ranges registered to and used by known banks and similar organisations. This information may be obtained directly from the organisations concerned. Since this information may change over time as new domain names and IP addresses are allocated, it is necessary to update the information regularly.

To achieve this, the system may regularly look up the IP addresses associated with known domain names and add them to the IP address list if not already there. Furthermore, the system may use the IP registration information held in the security information database 20 (as described above)

to search for new IP addresses or address ranges registered to known organisations, for example by comparing the name and address details of known organisations to the IP registration entries. If IP addresses are identified which are registered to a known organisation, these are added to the IP address list. Likewise, domain registration information may also be obtained and inspected to find newly registered domains.

In this way, an automatic update procedure may be provided to ensure that the lists of known "safe" domain names and IP address ranges remain up-to-date. This procedure may also be used when first populating the database. However, there may be a danger that such an automatic system could be abused, for example by an attacker registering a domain or IP address range using the name and address of a genuine organisation. To alleviate this problem, manual checks may be introduced whereby an operator checks the registration data, for example by telephoning the telephone number specified in the data and/or asking the organisation for confirmation of the registration, before a domain name or IP address is added to the safe list.

Since it will be in the banks' interests to keep their domain name and IP address information on the safe lists, it can be expected that they will endeavour to provide updated information to the provider / operator of the toolbar. This information can then be manually added to the database. Also, new banks or banks whose details do not yet appear on the safe lists may typically provide their information directly to the operator of the system for addition to the database, as otherwise their web sites may not be trusted by users of the toolbar.

Where the toolbar is provided by a particular banking organisation, the system may store only that particular bank's domain names and IP address ranges.

This system may be applied to web sites other than banking or financial web sites. For example, a "safe Internet shopping" icon could be provided which is displayed on the toolbar whenever a trusted Internet shopping web site is visited by the user. Generally speaking, the system may be applied to the kinds of web sites which are likely to be victims of "phishing" attacks, typically those which allow users to administer money or other tokens

of value, or which handle sensitive personal information (such as credit card details).

As an additional feature, the security information server can maintain a log of URLs (or representations thereof) visited by users of the system, from which aggregated reports can be produced about the behaviour of the user community in the aggregate. The toolbar provider can thereby obtain valuable information about the behaviour of their customers on the World Wide Web.

In conclusion, important aspects of the security system described include:

- Trapping of suspicious URLs containing characters which have no common purpose other than to deceive.
- Convenience of reporting the fraud to the bank and to the hosting location.
- Community watch behaviour of the system making warnings about fraudulent URLs immediately available to the rest of the community via display on the toolbar. Supervisor validation or a voting system can be used to reduce and eliminate the impact of false reporting of URLs.
- Clear display of sites' hosting location at all times while the user browses the web.
- Indication of security vulnerabilities on sites visited.
- Augmenting fraud fighting functionality with branding and marketing to help the bank or other organisation communicate to its customers, by offering more expedient navigation to its own services, and to bring new information and offers to the attention of its customers.
- Census quality information available to the bank or other organisation to learn about the web browsing behaviour of its customers in aggregate.

Adoption of the system could potentially change the chances of a successful fraud in the victims' favour and enable the banks' and other organisations' customers to defend themselves against fraud, as the user community is empowered to leverage the intellect and alertness of its most able members.

It will be understood that the present invention has been described above purely by way of example, and modification of detail can be made within the scope of the invention.

For example, specific processing described above as being performed at the user terminal by the toolbar could alternatively be performed by the security information server and vice versa. As an example of this, the security information server could perform all URL checking tasks including the character pattern matching. Alternatively, the toolbar could perform both the local and remote checks described above by maintaining a list of potentially dangerous URLs, which is periodically updated from the security information server. In that case, the toolbar could still request additional security information from the security information server (such as the hosting location and vulnerability information described above), possibly under control of the information button on the toolbar.

Instead of a toolbar which is integrated into the web browser software, a separate software component could also be used which intercepts URL requests output by the browser. This could, for example, work at the operating system level. Alternatively, a URL rewriting proxy could also fulfil the functionality of the toolbar, and provide facilities independent of particular operating system and browser software.

Each feature disclosed in the description, and (where appropriate) the claims and drawings may be provided independently or in any appropriate combination.

CLAIMS

1. A security component for use with an Internet browser application which displays Internet resources in response to receiving resource locators specifying the Internet resources; the security component comprising means for receiving a resource locator from the browser application and means for providing a security alert if the resource locator fulfils one or more criteria.

2. A component according to Claim 1, further comprising means for comparing the resource locator to a character pattern.

3. A component according to Claim 2, wherein the comparing means comprises means for testing the resource locator for the presence of one or more characters specified by the character pattern.

4. A component according to Claim 2 or 3, further comprising means for storing a plurality of character patterns.

5. A component according to Claim 4, further comprising means for receiving pattern update information; and means for updating character patterns stored in the storing means in response to the update information.

6. A component according to any of the preceding claims, further comprising means for transmitting a representation of the resource locator to a security information server, and means for receiving security information relating to the resource locator from the security information server.

7. A component according to Claim 6, wherein the security information comprises an indicator indicating whether the resource locator has been identified as being associated with a potential security risk, and wherein the criteria comprise the indicator.

8. A component according to Claim 6 or 7, wherein the security information comprises an indicator indicating whether the resource locator is associated with a trusted Internet location, and wherein the criteria comprise the indicator.

9. A component according to any of Claims 6 to 8, further comprising means for displaying the security information.

10. A component according to any of the preceding claims, wherein the alerting means is adapted to prevent the Internet browser application from displaying the Internet resource specified by the resource locator.

11. A component according to any of the preceding claims, further comprising means for receiving an indication of a suspected security risk from a user of the Internet browser application relating to an Internet resource viewed by the user, and means for transmitting the indication to a security information server.

12. A security component for use with an Internet browser application which displays Internet resources in response to receiving resource locators specifying the Internet resources; the security component comprising means for receiving a resource locator from the browser application; means for transmitting a representation of the resource locator to a remote server; means for receiving IP registration information relating to the resource locator from the remote server; and means for displaying the IP registration information.

13. A plug-in for an Internet browser application comprising a component as claimed in any of Claims 1 to 12.

14. A toolbar for an Internet browser application comprising a component as claimed in any of Claims 1 to 12.

15. A security information server comprising:

a database of security information relating to Internet locations;

means for receiving a security information request comprising a representation of a resource locator from a user terminal;

means for retrieving security information relating to the resource locator from the database; and

means for transmitting the security information to the user terminal.

16. A security information server according to Claim 15, further comprising:

means for receiving security information relating to a specified resource locator from a user terminal; and means for updating the database in dependence on the security information received.

17. A security information server according to Claim 15 or 16, wherein the database is adapted to store a list of representations of resource locators having been identified as being associated with a potential security risk, the security information server further comprising means for comparing the received resource locator representation to the stored list of resource locator representations, the transmitted security information comprising an indicator indicating whether the received resource locator representation matches one of the stored list of resource locator representations.

18. A security information server according to Claim 17, further comprising means for receiving an indication of a suspected security risk relating to a specified resource locator from a user terminal; and means for adding a representation of the specified resource locator to the list.

19. A security information server according to any of Claims 15 to 18, wherein the database is adapted to store information relating to suspected security vulnerabilities associated with an Internet location.

20. A security information server according to Claim 19, further comprising means for assessing whether potential security vulnerabilities are associated with an Internet location.

21. A security information server according to Claim 20, wherein the assessing means is adapted to identify potential security vulnerabilities in dependence on one or more of: the operating system of a web server associated with the location, the version of that operating system, the web server software used by the web server, and the version of that web server software.

22. A security information server according to any of claims 15 to 21, wherein the database is adapted to store registration information relating to a plurality of IP addresses, and wherein the retrieving means is adapted to retrieve registration information relating to an IP address associated with the received resource locator representation.

23. A security information server according to Claim 22, wherein the registration information comprises information relating to the company or person to whom the IP address is registered.

24. A security information server according to any of Claims 15 to 23, wherein the database is adapted to store information relating to trusted Internet locations, the security information server further comprising means for determining whether the received resource locator representation relates to a trusted Internet location, the transmitted security information comprising an indicator indicating whether the received resource locator representation relates to a trusted Internet location.

25. A security information server according to Claim 24, wherein the information comprises a list of trusted domain names.

26. A security information server according to Claim 24 or 25, wherein the information comprises a list of trusted IP addresses or IP address ranges.

27. A security information system comprising a security information server as claimed in any of Claims 15 to 26 and a plurality of user terminals each comprising a security component as claimed in any of Claims 1 to 12.

28. A method of providing security information comprising:

receiving a representation of a resource locator relating to an Internet resource requested by a user of an Internet browser application; and

alerting the user if the resource locator representation fulfils one or more criteria.

29. A method according to Claim 28, further comprising comparing the resource locator representation to a character pattern, the alerting step comprising alerting the user in dependence on the outcome of the comparison.

30. A method according to Claim 29, wherein the comparing step comprises testing the resource locator representation for the presence of one or more characters specified by the character pattern.

31. A method according to Claim 29 or 30, further comprising storing a plurality of character patterns.

32. A method according to Claim 31, further comprising receiving pattern update information; and updating the plurality of stored character patterns in response to the update information.

33. A method according to any of Claims 28 to 32, further comprising:

maintaining a database of security information relating to Internet locations; and

retrieving security information relating to the received resource locator representation from the database; the alerting step comprising alerting the user in dependence on the security information.

34. A method according to Claim 33, further comprising: storing a list of representations of resource locators having been identified as being associated with a potential security risk in the database; and comparing the received resource locator representation to the stored list of resource locator representations; the alerting step comprising alerting the user in dependence on the outcome of the comparison.

35. A method according to Claim 34, further comprising receiving an indication of a suspected security risk relating to a specified resource locator from a user; and adding a representation of the specified resource locator to the list.

36. A method according to any of Claims 33 to 35, further comprising storing information relating to suspected security vulnerabilities associated with an Internet location in the database.

37. A method according to Claim 36, further comprising assessing an Internet location to determine whether potential security vulnerabilities are associated with the location, and storing the outcome of the assessment in the database.

38. A method according to Claim 37, wherein the assessing step comprises identifying potential security vulnerabilities in dependence on one or more of: the operating system of a web server associated with the location, the version of that operating system, the web server software used by the web server, and the version of that web server software.

39. A method according to any of Claims 33 to 38, further comprising storing registration information relating to a plurality of IP addresses in the database, and wherein the retrieving step comprises

retrieving registration information relating to an IP address associated with the received resource locator representation.

40. A method according to any of Claims 33 to 39, further comprising storing information relating to trusted Internet locations, and determining whether the received resource locator representation relates to a trusted Internet location; the alerting step comprising alerting the user in dependence on the outcome of the determination.

41. A method according to Claim 40, wherein the information comprises a list of trusted domain names.

42. A method according to Claim 40 or 41, wherein the information comprises a list of trusted IP addresses or IP address ranges.

43. A method according any of Claims 33 to 42, further comprising displaying the security information.

44. A method according to any of Claims 28 to 43, wherein the alerting step comprises preventing the Internet browser application from displaying the Internet resource specified by the resource locator.

45. A method of providing security information to a user accessing via the Internet accounts for holding or managing money or other tokens of value, comprising:

storing domain names and/or IP address information relating to trusted Internet sites providing access to such accounts;

receiving a resource locator specifying an Internet resource requested by the user;

determining whether the resource locator relates to a trusted Internet site by comparing a domain name or IP address associated with the resource locator to the stored domain names and/or IP address information; and

outputting a corresponding indication to the user if it is determined that the resource locator does relate to a trusted Internet site.

46. A component, plug-in or toolbar for an Internet browser application adapted to carry out a method as claimed in any of Claims 28 to 45.

47. A security information server adapted to carry out a method as claimed in any of Claims 28 to 45.

48. A component, plug-in or toolbar for use with an Internet browser application substantially as described herein with reference to and as illustrated in Figures 1 to 5 of the accompanying drawings.

49. A security information server substantially as described herein with reference to and as illustrated in Figures 1, 2 and 6 of the accompanying drawings.

50. A security system substantially as described herein with reference to and as illustrated in Figures 1 to 6 of the accompanying drawings.

51. A method of providing security information substantially as described herein with reference to and as illustrated in Figures 1 to 6 of the accompanying drawings.

ABSTRACT

SECURITY COMPONENT FOR USE WITH AN INTERNET BROWSER APPLICATION AND METHOD AND APPARATUS ASSIATED THEREWITH

A security component for use with an Internet browser application which displays Internet resources in response to receiving resource locators specifying the Internet resources is disclosed. The security component comprises means for receiving a resource locator from the browser application and means for providing a security alert if the resource locator fulfils one or more criteria. The security component may be a plug-in or toolbar for a web browser application. A security information server and a method of providing security information are also disclosed.

(Figure 2)

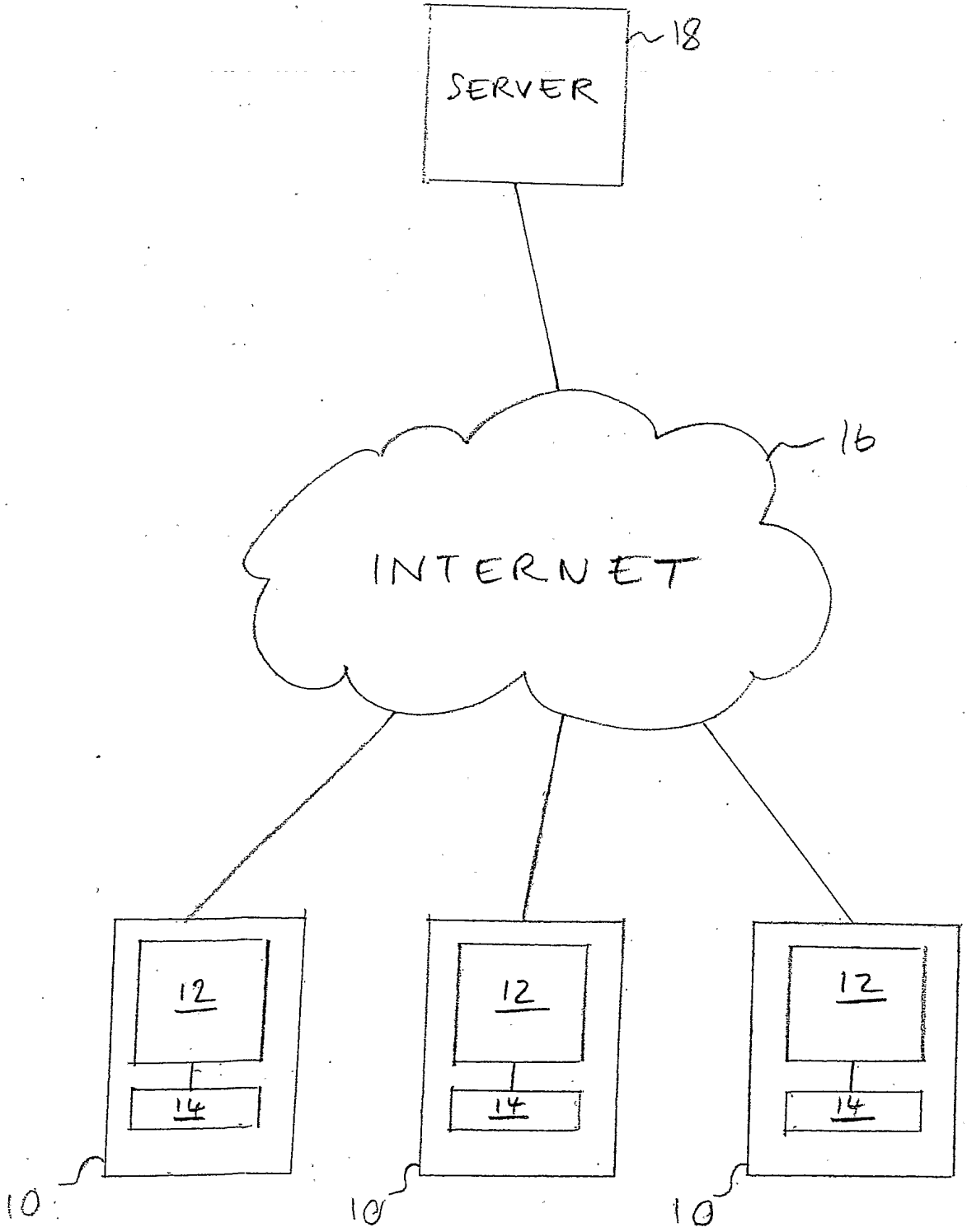


FIG. 1

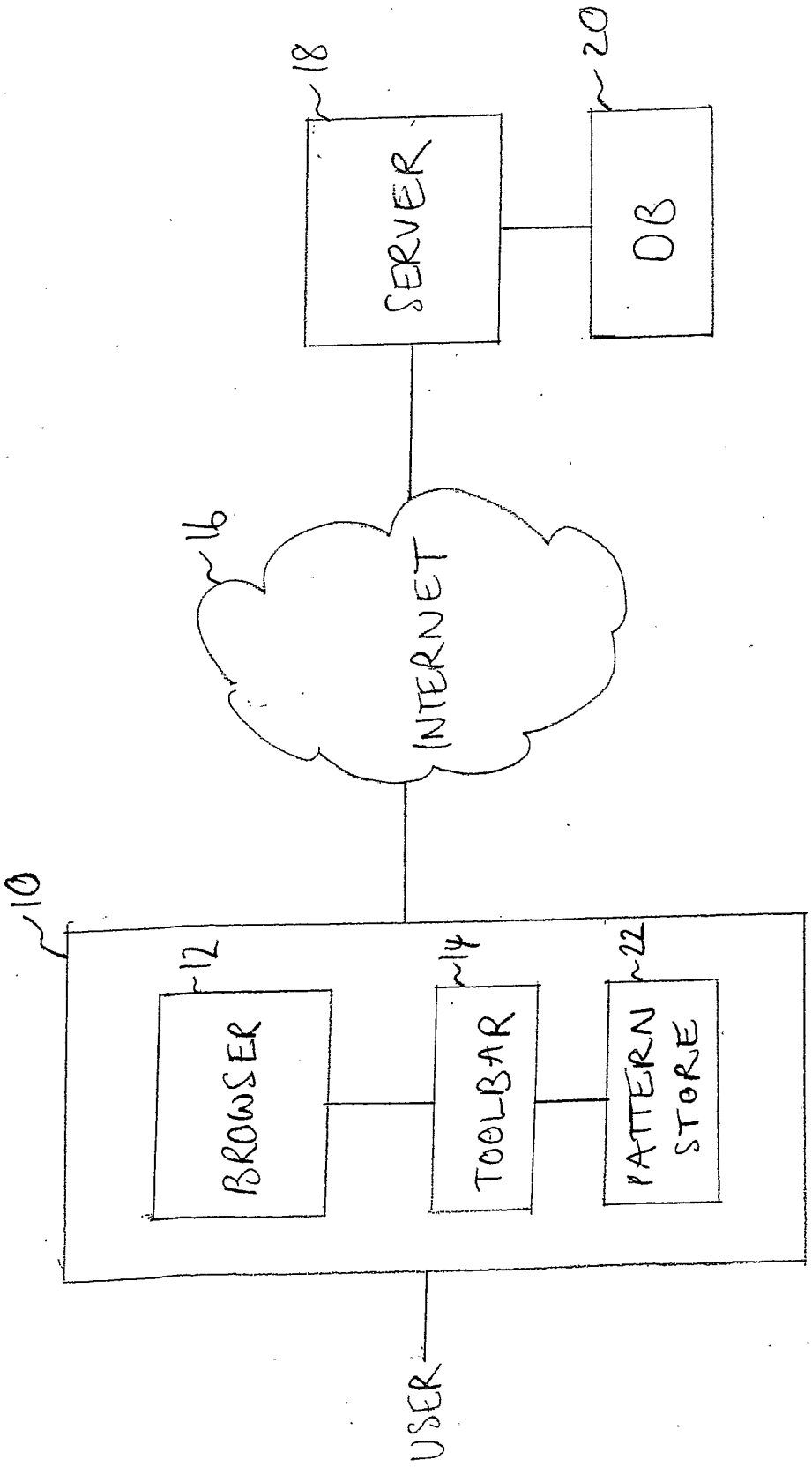

18
SERVER
20
DB
16
INTERNET
10
12
BROWSER
14
TOOLBAR
22
PATTERN STORE
USER

FIG. 2

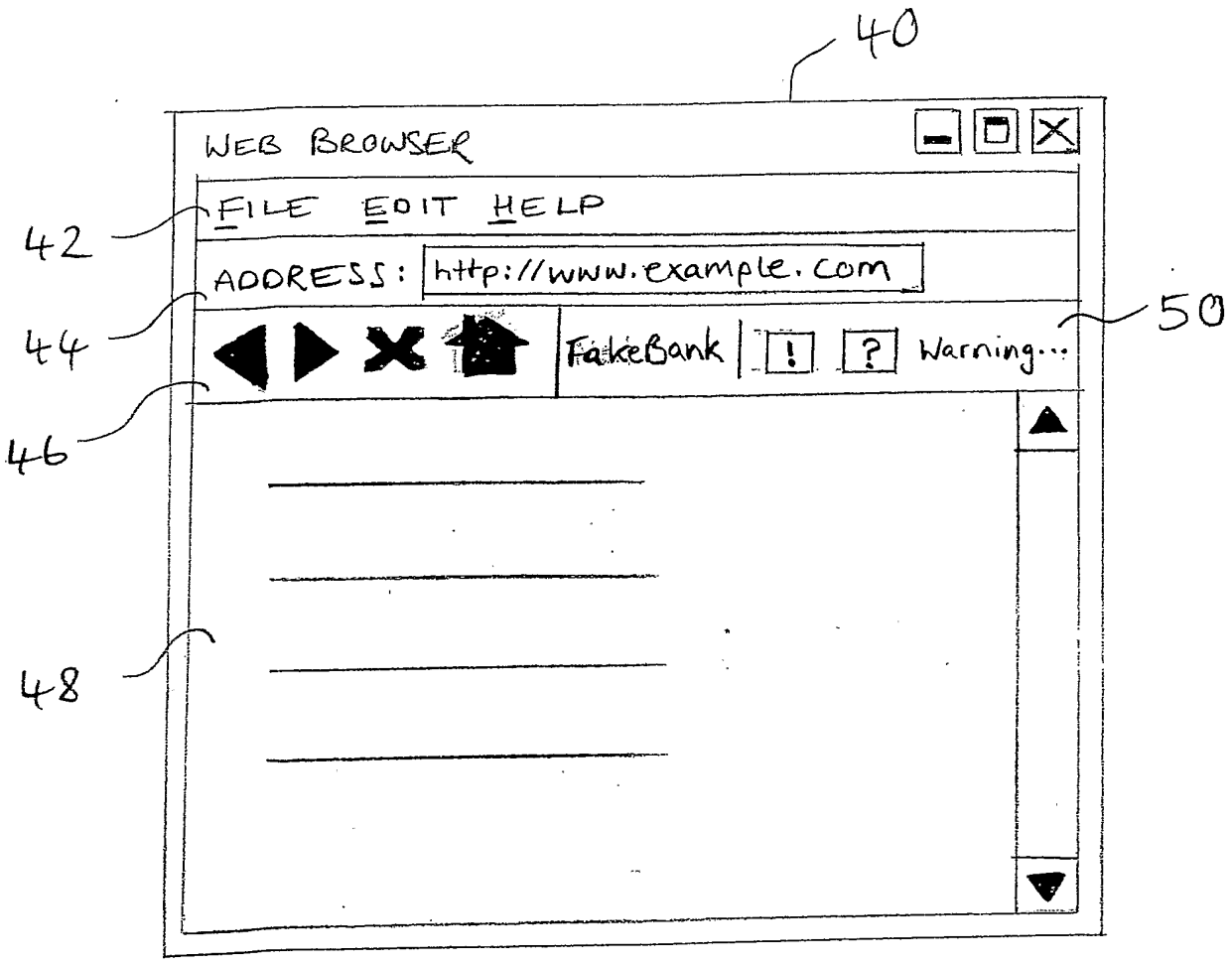

40
WEB BROWSER
FILE EDIT HELP
42
ADDRESS: http://www.example.com
44
FakeBank
!
?
Warning...
50
46
48

FIG. 3

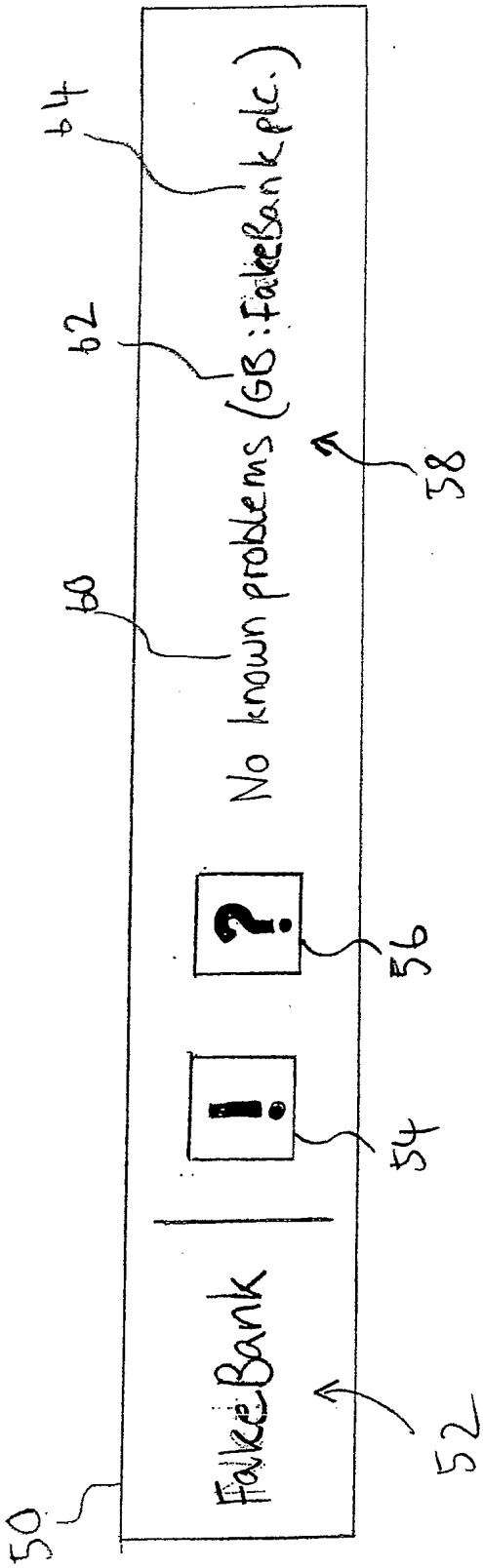

50
FakeBank
52
54
56
No known problems (GB: FakeBank plc.)
58
60
62
64

FIG. 4

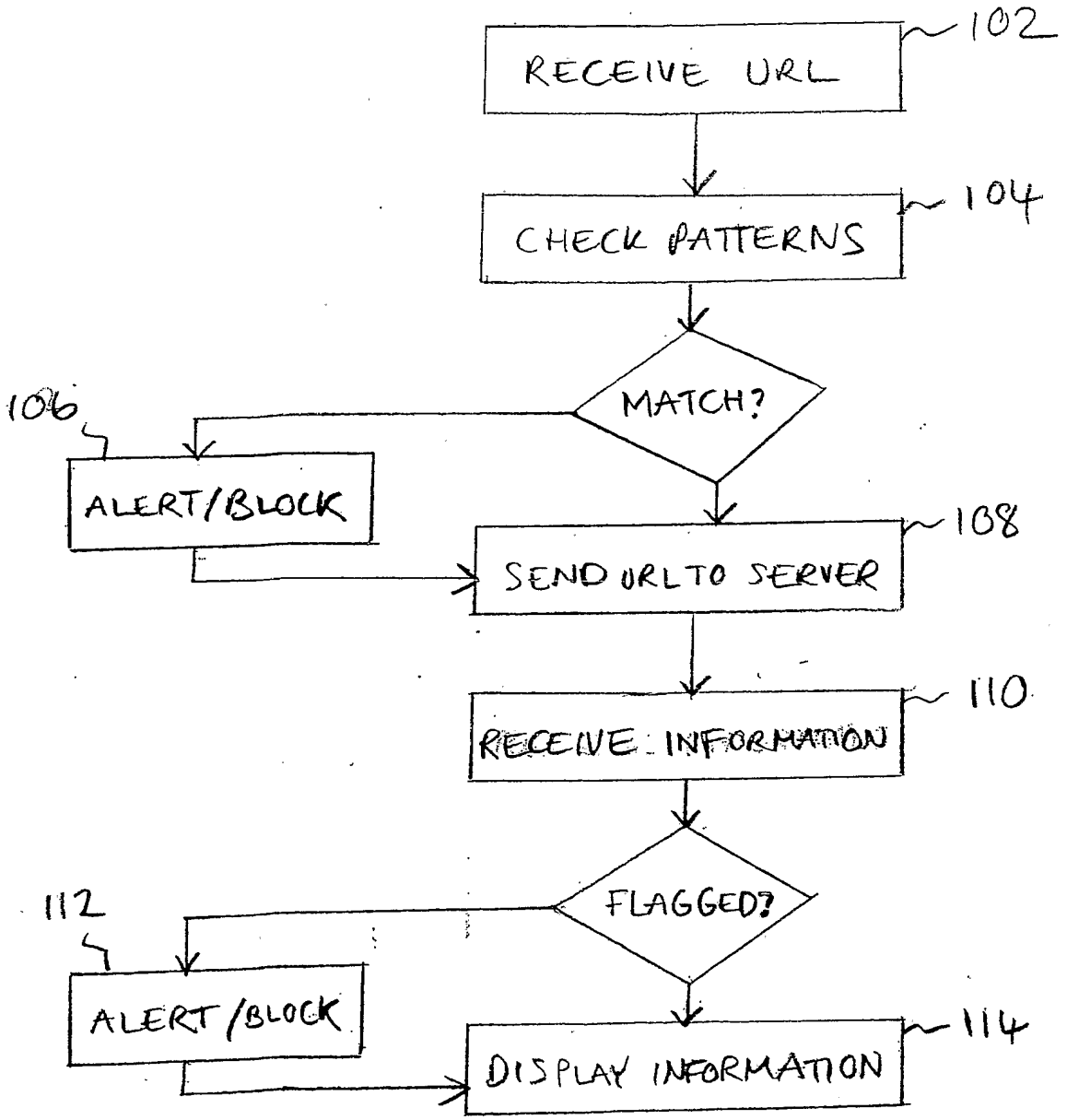

RECEIVE URL
102
CHECK PATTERNS
104
MATCH?
106
ALERT/BLOCK
SEND URL TO SERVER
108
RECEIVE INFORMATION
110
FLAGGED?
112
ALERT/BLOCK
DISPLAY INFORMATION
114

FIG. 5

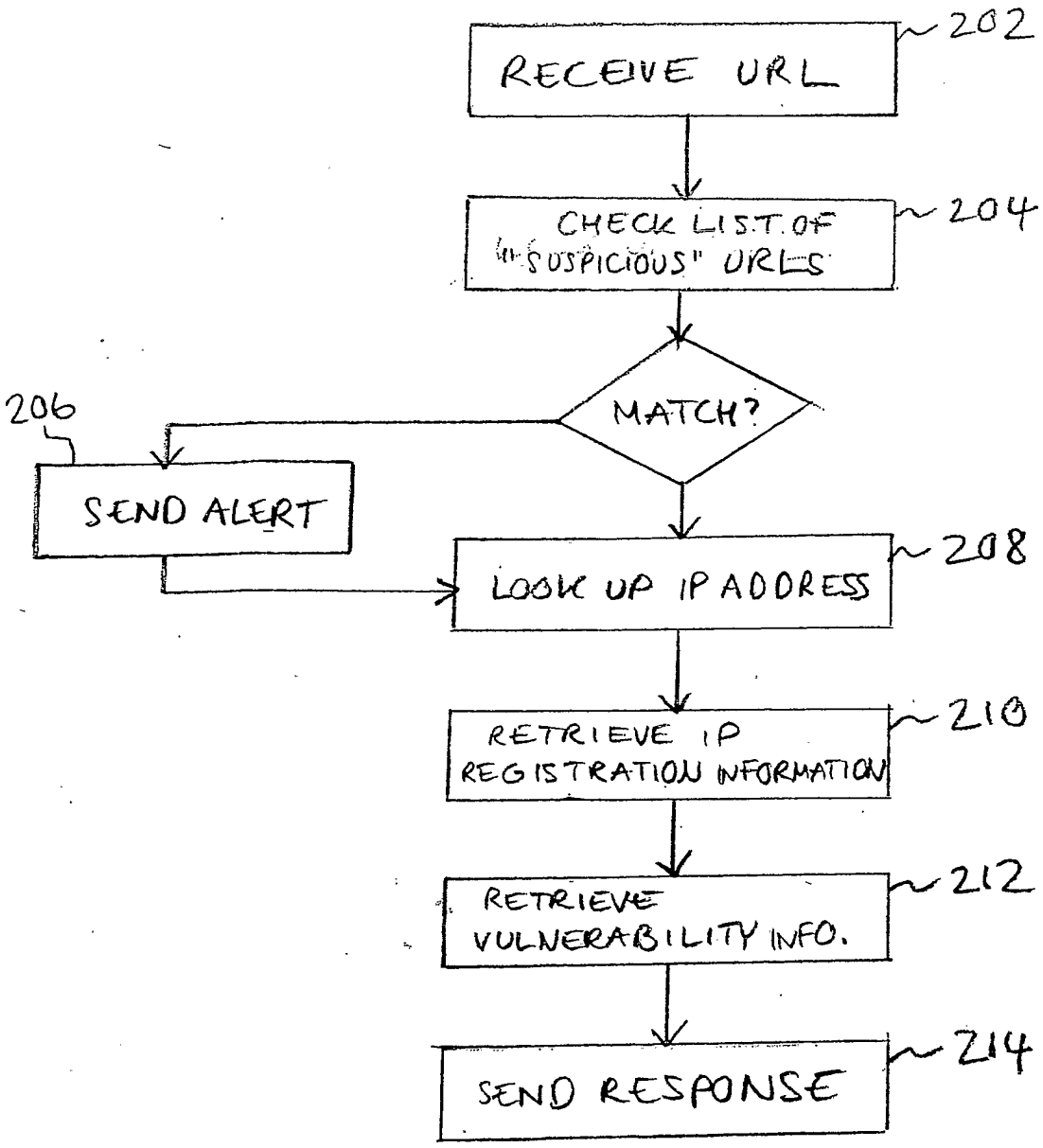

RECEIVE URL
202
CHECK LIST OF "SUSPICIOUS" URLS
204
MATCH?
206
SEND ALERT
LOOK UP IP ADDRESS
208
RETRIEVE IP REGISTRATION INFORMATION
210
RETRIEVE VULNERABILITY INFO.
212
SEND RESPONSE
214

FIG. 6

PCT/GB2005/000978

15/3/05

MATHS SQUARE.